Key Rate of the B92 Quantum Key Distribution Protocol with Finite Qubits

Hiroaki Sasaki*, Ryutaroh Matsumoto*, and Tomohiko Uyematsu*
*Department of Communications and Computer Engineering, Tokyo Institute of Technology, Japan.

***Abstract*—The key rate of the B92 quantum key distribution protocol had not been reported before this research when the number of qubits is finite. We compute it by using the security analysis framework proposed by Scarani and Renner in 2008.**

***Keywords*—B92, quantum key distribution**

I. Introduction

The B92 quantum key distribution (QKD) protocol [2] has remained less popular than the famous BB84 protocol [1], while both protocols provide the unconditional security. One plausible reason for the unpopularity is that the B92 is weaker to the channel noise than the BB84. Specifically, the BB84 with the standard one-way information reconciliation can generate secure key over the depolarizing channel at depolarizing rate 16.5%, while the previous security analyses of the B92 cannot guarantee the secure key generation at depolarizing rate 3.5% [13], 3.7% [4] or 4.2% [10]. By using the security analysis framework introduced by Renner in 2005 [9], we improved the maximal tolerable depolarizing rate to 6.5% [7].

All of the above analyses [4], [7], [10], [13] assumed the infinite number of qubits in the protocol, and derived the asymptotic key rates. On the other hand, in practice the number of qubits used in a protocol is always finite. However, before this research, the key rates with finite qubits in the B92 protocol had not been reported, as far as the authors know. In this paper, we report the key rates with finite qubits, based on the analytic framework introduced by Scarani and Renner [12] and our previous researches [7], [11]. We stress that the assumption in our paper is the same as [12], and in particular we assume the collective attack instead of the coherent attack.

II. New Security Analysis of the B92 Protocol with Finite Qubits

In this section, we present a new formula for the key rate of the B92 protocol with finite qubits, based on previous researches [7], [11], [12]. The following description has some overlap with our previous research improving the asymptotic key rate of the B92 [7]. Firstly, we fix notations. Let $\{|0\rangle, |1\rangle\}$ be some fixed orthonormal basis of a qubit. In the B92 protocol [2], Alice sends the quantum state

$$|\varphi_j\rangle = \beta|0\rangle + (-1)^j\alpha|1\rangle, \tag{1}$$

for $j = 0, 1$, where $\beta = \sqrt{1-\alpha^2}$, and $0 < \alpha < 1/\sqrt{2}$. For convenience of presentation, we also define

$$|\bar{\varphi}_j\rangle = \alpha|0\rangle - (-1)^j\beta|1\rangle.$$

We can see that $\{|\varphi_j\rangle, |\bar{\varphi}_j\rangle\}$ forms an orthonormal basis of a qubit.

On the other hand, we can express a qubit channel as follows. Define the three Pauli matrices σ_x, σ_y, and σ_z as usual. Then a qubit density matrix ρ can be expressed as [8]

$$\rho = \frac{1}{2}\left(I + x\sigma_x + y\sigma_y + z\sigma_z\right),$$

where $x, y, z \in \mathbf{R}$ and $x^2 + y^2 + z^2 \leq 1$. The vector (x, y, z) is called a Bloch vector. The qubit channel $\mathcal{E}_B$ from Alice to Bob can be expressed [6] as a map between Bloch vectors by

$$\begin{pmatrix} z \\ x \\ y \end{pmatrix} \mapsto R\begin{pmatrix} z \\ x \\ y \end{pmatrix} + \vec{t}, \tag{2}$$

where

$$R = \begin{pmatrix} R_{zz} & R_{zx} & R_{zy} \\ R_{xz} & R_{xx} & R_{xy} \\ R_{yz} & R_{yx} & R_{yy} \end{pmatrix}, \quad \vec{t} = \begin{pmatrix} t_z \\ t_x \\ t_y \end{pmatrix}. \tag{3}$$

Define

$$|\Psi\rangle = \frac{|0\rangle_A|\varphi_0\rangle_B + |1\rangle_A|\varphi_1\rangle_B}{\sqrt{2}}.$$

As in [13], we also define the four POVM

$$F_0 = |\bar{\varphi}_1\rangle\langle\bar{\varphi}_1|/2, \tag{4}$$
$$F_1 = |\bar{\varphi}_0\rangle\langle\bar{\varphi}_0|/2, \tag{5}$$
$$F_{\bar{0}} = |\varphi_1\rangle\langle\varphi_1|/2, \tag{6}$$
$$F_{\bar{1}} = |\varphi_0\rangle\langle\varphi_0|/2. \tag{7}$$

In [13], the measurement outcomes corresponding to $F_{\bar{0}}$ and $F_{\bar{1}}$ was not distinguished. We distinguish them for better channel estimation.

After passing the quantum channel $\mathcal{E}_B$ from Alice to Bob, $|\Psi\rangle\langle\Psi|$ becomes

$$\rho_{1,AB} = (I \otimes \mathcal{E}_B)|\Psi\rangle\langle\Psi|. \tag{8}$$

In a quantum key distribution protocol, the state change $\mathcal{E}_B$ is caused by Eve's cloning of the transmitted qubits to her quantum memory. The content of Eve's quantum memory is mathematically described by the purification $|\Phi_{1,ABE}\rangle$ of $\rho_{1,AB}$. Let $\rho_{1,ABE} = |\Phi_{1,ABE}\rangle\langle\Phi_{1,ABE}|$.

In addition to Eve's quantum memory, she also knows the content of public communication over the classical public channel between Alice and Bob. For each transmitted qubit from Alice to Bob, the public communication consists of 1-bit information indicating whether Bob excludes his received

qubit for generating the final secret key or not. We also have to take it into account. We shall represent the public communication by a classical random variable P that becomes 1 if Bob excludes his qubit and 0 otherwise. So, $P = 0$ when Bob's measurement outcome is F_0 or F_1, and $P = 1$ when Bob's measurement outcome is $F_{\bar{0}}$ or $F_{\bar{1}}$.

On the other hand, in the B92 protocol, Bob performs the measurement specified by Eqs. (4)–(7). Alice and Bob use their qubit for generation of the final secret key only if its measurement outcome is F_0 or F_1. Otherwise it is excluded from the key generation. This is mathematically equivalent to set Alice's bit to 0 if the measurement outcomes is $F_{\bar{0}}$ or $F_{\bar{1}}$. Therefore, from Eve's perspective on Alice's classical bit, the joint state between Alice and Bob after the selection by measurement outcomes is equivalent to

$$\begin{aligned}\rho_{2,ABEP} &= (I_A \otimes \sqrt{F_0} \otimes I_E \rho_{1,ABE} I_A \otimes \sqrt{F_0} \otimes I_E \\ &\quad + I_A \otimes \sqrt{F_1} \otimes I_E \rho_{1,ABE} I_A \otimes \sqrt{F_1} \otimes I_E) \otimes |0\rangle_P\langle 0|_P \\ &\quad + |0\rangle_A\langle 0|_A \otimes (\sqrt{F_{\bar{0}}} \otimes I_E \mathrm{Tr}_A[\rho_{1,ABE}] \sqrt{F_{\bar{0}}} \otimes I_E \\ &\quad + \sqrt{F_{\bar{1}}} \otimes I_E \mathrm{Tr}_A[\rho_{1,ABE}] \sqrt{F_{\bar{1}}} \otimes I_E) \otimes |1\rangle_P\langle 1|_P.\end{aligned}$$

Observe that the state change from $\rho_{1,ABE}$ to $\rho_{2,ABEP}$ is a trace-preserving completely positive map.

In order to calculate the key rate, we need to consider Eve's ambiguity on Alice's classical bit [10], [9] defined as follows. Let

$$\rho_{2,XEP} = \sum_{j=0,1} |j\rangle_A\langle j|_A \otimes I_{EP} \mathrm{Tr}_B[\rho_{2,ABEP}] |j\rangle_A\langle j|_A \otimes I_{EP}.$$

Eve's ambiguity on Alice's classical bit $S(X|EP)$ is defined as

$$S(X|EP) = S(\rho_{2,XEP}) - S(\rho_{2,EP}), \tag{9}$$

where $\rho_{2,EP} = \mathrm{Tr}_A[\rho_{2,XEP}]$, and $S(\cdot)$ denotes the von Neumann entropy.

In order to calculate the amount of public communication required for information reconciliation, we define the joint random variables (X', Y') as

$$\begin{aligned} X' &= j \text{ if the transmitted qubit is } |\varphi_j\rangle, \\ Y' &= k \text{ if the measurement outcome is } F_k, \end{aligned} \tag{10}$$

under the condition that the measurement outcome is either F_0 or F_1. Observe the difference between X and X'. X' is not defined but X is defined to be 0 when Bob's measurement outcome is either $F_{\bar{0}}$ or $F_{\bar{1}}$.

We shall show the key rate per single transmitted qubit that is neither announced for the channel estimation nor excluded due to the measurement outcome being $F_{\bar{0}}$ or $F_{\bar{1}}$. Note that Eq. (9) is Eve's ambiguity per a qubit that is not announced for the channel estimation but *can be discarded*. The probability of the measurement outcome being F_0 or F_1 is

$$\mathrm{Tr}[\rho_{1,AB}(I_A \otimes (F_0 + F_1))].$$

So we can see that Eve's ambiguity per single transmitted qubit that is neither announced for the channel estimation nor discarded is

$$\frac{S(X|EP)}{\mathrm{Tr}[\rho_{1,AB}(I \otimes (F_0 + F_1))]}.$$

By [10], [9] the *asymptotic* key rate is

$$\frac{S(X|EP)}{\mathrm{Tr}[\rho_{1,AB}(I \otimes (F_0 + F_1))]} - H(X'|Y'). \tag{11}$$

The above analysis is almost the same as our previous one [7] for the asymptotic key rate assuming the infinite number of qubits.

Note that the above formula (11) assumes that Alice and Bob know the channel between them. In the BB92 protocol, we cannot estimate all the parameters of the channel, even if we assume infinitely many qubits in the protocol. We can only estimate part of them. In addition to that, because the number of qubits in the protocol is finite, there must be statistical errors.

To handle the finiteness of qubits, Scarani and Renner [12] used the interval estimation of channel parameters (R and $\vec{t}$ of (3) in our study). In contrast to the more popular point estimation, by using statistical samples, interval estimation gives a set of parameters that contains true parameters with high probability $1 - \epsilon_{\mathrm{PE}}$. By using the results in [12], the key rate of the B92 protocol can be computed as

$$r = \min_{(R,\vec{t}) \in \Gamma(\epsilon_{\mathrm{PE}})} S(X|EP) - H(X'|Y') - \Delta/n, \tag{12}$$

where $\Gamma(\epsilon_{\mathrm{PE}})$ is a confidence region given by an interval estimation procedure with the confidence level $\geq 1 - \epsilon_{\mathrm{PE}}$, Δ is as defined in [12, Eq. (5)], and n is the number of the qubits to which Alice and Bob apply the privacy amplification.

To compute the rate (12), there are two remaining tasks, namely (a) computation of $\Gamma(\epsilon_{\mathrm{PE}})$, and (b) computation of $\min_{(R,\vec{t}) \in \Gamma(\epsilon_{\mathrm{PE}})} S(X|EP)$. Task (b) is performed by using the convex optimization method [3] as done in our previous researches [7], [11]. For convex optimization, the confidence region $\Gamma(\epsilon_{\mathrm{PE}})$ must be a convex set that can be easily handled by a mathematical software, like Mathematica. In [11], such a convex confidence region was introduced for the BB84 protocol by using the KL divergence. We shall define $\Gamma(\epsilon_{\mathrm{PE}})$ also by using the KL divergence.

In the conventional researches [4], [7], [10], [13], their channel estimation procedures classified Bob's measurement outcomes into three categories, namely, F_0, F_1 and the inconclusive ($F_{\bar{0}}$ or $F_{\bar{1}}$). In this research, we propose to distinguish $F_{\bar{0}}$ and $F_{\bar{1}}$ for better estimation accuracy. On the other hand, the conventional estimation procedures did not distinguish which $|\varphi_0\rangle$ or $|\varphi_1\rangle$ produced Bob's measurement outcome. We also propose to distinguish Alice's transmitted qubits $|\varphi_0\rangle$ and $|\varphi_1\rangle$ in channel estimation.

By the above consideration, the proposed channel estimation procedure has at least 8 kinds of outcomes. On the other hand, the treatment of Bob's outcome F_0, F_1, $F_{\bar{0}}$ and $F_{\bar{1}}$ is asymmetric, because all of $F_{\bar{0}}$ and $F_{\bar{1}}$ are disclosed to Alice and are used for channel estimation, while parts of F_0 and F_1 are kept secret for the secret key generation. Because of this asymmetry, the sum of 8 POVM operators corresponding the above 8 outcomes does not become the 4×4 identity matrix $I_{4\times 4}$. To make the sum equal to $I_{4\times 4}$, we include the outcome meaning the qubit kept secret for secret key generation. By

$r_{pub}(0 < r_{pub} < 1)$ we denote the conditional probability for a qubit being disclosed for channel estimation, and the qubit is kept secret for secret key generation with a probability r_{pub}. We define the following 8 POVM operators:

$$E_0 = r_{pub}|0_A\rangle\langle 0_A| \otimes F_0 \quad (13)$$
$$E_1 = r_{pub}|0_A\rangle\langle 0_A| \otimes F_1 \quad (14)$$
$$E_2 = |0_A\rangle\langle 0_A| \otimes F_{\bar{0}} \quad (15)$$
$$E_3 = |0_A\rangle\langle 0_A| \otimes F_{\bar{1}} \quad (16)$$
$$E_4 = r_{pub}|1_A\rangle\langle 1_A| \otimes F_0 \quad (17)$$
$$E_5 = r_{pub}|1_A\rangle\langle 1_A| \otimes F_1 \quad (18)$$
$$E_6 = |1_A\rangle\langle 1_A| \otimes F_{\bar{0}} \quad (19)$$
$$E_7 = |1_A\rangle\langle 1_A| \otimes F_{\bar{1}} \quad (20)$$
$$E_8 = (1 - r_{pub})I_{2\times 2} \otimes (F_0 + F_1). \quad (21)$$

The last operator E_8 corresponds to the imaginary measurement outcome expressing the non-disclosure of a qubit.

By this preparation of notations, we can describe the proposed confidence region of the channel parameters. Let $D(P\|Q)$ denotes the Kullback-Leibler divergence, $\lambda(\rho_{1,AB})$ the theoretical probability distribution of the 9 outcomes defined as

$$\lambda_\infty(\rho_{1,AB}) = (\mathrm{Tr}[\rho_{1,AB}E_0], \ldots, \mathrm{Tr}[\rho_{1,AB}E_8]),$$

and λ_m the empirical distribution (i.e. relative frequencies) of the 9 outcomes, where m is the total number of qubits transmitted including both disclosed and non-disclosed qubits. Observe that Alice and Bob can compute λ_m in the protocol execution, and their task is to estimate the channel parameters $(R, \vec{t})$. The set

$$\{(R,\vec{t}) \mid D(\lambda_m\|\lambda_\infty(\rho_{1,AB})) \le \epsilon_{\mathrm{PE}}, (R,\vec{t}) \text{ defines a CP map}\} \quad (22)$$

is a confidence region of $(R, \vec{t})$ with confidence level at least $1 - \epsilon_{\mathrm{PE}}$, by the well-known fact [5, Theorem 11.2.1]. It is also well-known that the set of $(R, \vec{t})$ yielding a CP map is convex [6], and $D(\cdot\|\cdot)$ is a convex function. Therefore the set (22) is a convex set. The above idea is similar to our previous research [11] on BB84. We have verified that the set (22) can be used as $\Gamma(\epsilon_{\mathrm{PE}})$ in (12).

The minimization in (12) is just a convex optimization and can be done as follows. Observe first that $S(X|EP)$ is a function of the channel parameters (3) of $\mathcal{E}_B$. By the almost same argument as [14, Remark 11] one sees that $S(X|EP)$ is a convex function of the channel parameters (3). Moreover, we see that the minimum of $S(X|EP)$ is attained when $R_{xy} = R_{yx} = R_{yz} = R_{zy} = t_y = 0$ by the almost same argument as [14, Proposition 1]. Therefore, one can compute the minimization of $S(X|EP)$ by the convex optimization [3].

III. Numerical Result

We consider the depolarizing channel $\mathcal{E}_q$ with depolarizing rate q. The definition of q follows [13]. For a qubit density matrix ρ, we have $\mathcal{E}_q(\rho) = (1 - q)\rho + (q/2)I_{2\times 2}$. With such a channel $\mathcal{E}_q$, R and $\vec{t}$ in Eq. (2) are given by

$$R = \begin{pmatrix} 1-4q/3 & 0 & 0 \\ 0 & 1-4q/3 & \\ 0 & 0 & 1-4q/3 \end{pmatrix}, \quad \vec{t} = \vec{0}.$$

We stress that we do not restrict the range of minimization in (12) to the depolarizing or the Pauli channels. The minimization is carried out over the set of all the qubit channels in (22). The FindMinimum function in Mathematica 9.0 was used for the minimization.

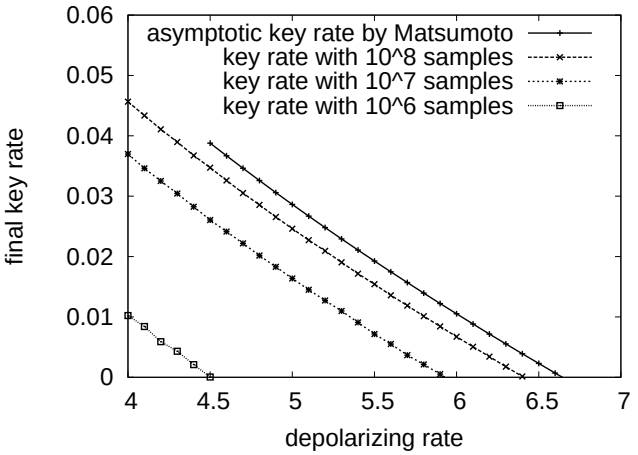

Fig. 1. Key rates with various depolarizing rates of the quantum channel

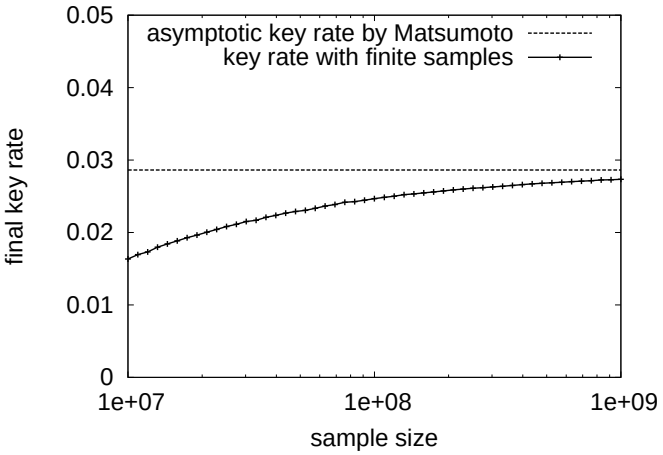

Fig. 2. Key rates with various sample sizes (depolarizing rate is 5%)

In Fig. 1, the key rates for various depolarizing rates are plotted, and we compare key rates by our proposal and the asymptotic rates by Matsumoto [7]. We can observe that positive key rate is achieved at depolarizing rate 6.4% with 10^8 samples. The sample size refers to the total number m of transmitted qubits from Alice to Bob, including qubits giving measurement outcomes $F_{\bar{0}}$ and $F_{\bar{0}}$ and qubits becoming sifted key. In Fig. 2, the key rates for various sample sizes are plotted with a fixed depolarizing rate 5%, and we also compare key rates by our proposal and the asymptotic rates by Matsumoto [7]. We can observe that our key rates converge to the asymptotic one. We only considered $\alpha = 0.39$ and did

not optimize the value of α in Eq. (1). The value $\alpha = 0.39$ was also used in [7]. r_{pub} was always set to 0.5 in our numerical computation.

IV. Conclusion

Before this research, the secure key rate of the B92 quantum key distribution protocol had not been reported. We have clarified it. Our analysis is based on the finite key rate formula proposed by Scarani and Renner [12] combined with our previous researches [7], [11]. We have shown that one can have a positive key rate with 10^8 samples over a depolarizing channel with depolarizing rate 6.4%.

Acknowledgment

The authors would like to thank Prof. Shun Watanabe for his helpful comments. This research is partly supported by the NICT and the JSPS Grants No. 23246071. This research is in part carried out during the second author's stay in Aalborg university that was supported by the Villum Foundation through their VELUX Visiting Professor Programme 2013–2014.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Intl. Conf. on Computers, Systems, and Signal Processing*, 1984, pp. 175–179.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[3] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[4] M. Christandl, R. Renner, and A. Ekert, "A generic security proof for quantum key distribution," Mar. 2004, arXiv:quant-ph/0402131.

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley Interscience, 2006.

[6] A. Fujiwara and P. Algoet, "One-to-one parametrization of quantum channels," *Phys. Rev. A*, vol. 59, no. 5, pp. 3290–3294, May 1999.

[7] R. Matsumoto, "Improved asymptotic key rate of the B92 protocol," in *Proc. 2013 IEEE ISIT*, Istanbul, Turkey, Jul. 2013, pp. 351–353.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2000.

[9] R. Renner, "Security of quantum key distribution," *International Journal on Quantum Information*, vol. 6, no. 1, pp. 1–127, Feb. 2008, (originally published as Ph.D thesis, ETH Zürich, Switzerland, 2005).

[10] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, no. 1, p. 012332, Jul. 2005.

[11] Y. Sano, R. Matsumoto, and T. Uyematsu, "Secure key rate of the BB84 protocol using finite sample bits," *J. Phys. A: Math. Theor.*, vol. 43, no. 49, p. 495302, Nov. 2010.

[12] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Phys. Rev. Lett.*, vol. 100, no. 20, p. 200501, May 2008.

[13] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Phys. Rev. Lett.*, vol. 90, no. 16, p. 167904, Apr. 2003.

[14] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Phys. Rev. A*, vol. 78, no. 4, p. 042316, Oct. 2008.